"Anti-Terrorism Security 101"

By

Michael Minieri, CPP, CSC, CST, CCO, CET, CFPS, CPOI, CSM, RAM

Principle Security Consultant – www.MinieriAssociates.com

Around the time of this writing, we are - once again - seeing an increase in terrorist attacks around the globe. Presently, there is NO evidence at all to suggest that this threat will decrease in the foreseeable future, and it is much more likely that the opposite is true. Little information of any use regarding the physical security measures – if any – that were in place at the time of the attack can be extracted from news media reports. Most physical security professionals are probably curious about such things and for obvious reasons. Based upon 40+ years of global experience and observation at thousands of facilities, author Michael Minieri outlines some basic – but critical – considerations when establishing an effective security plan against terrorism for any type of facility.

THE TOP 3 GENERAL TERRORIST ATTACK STRATEGIES

1) SMALL ARMS ATTACK: One or more individuals enter the premises with firearms usually ranging from hand-guns to automatic weapons such as the ubiquitous AK-47. In addition to shooting occupants, taking hostages – sometimes many – is common.

2) PEDESTRIAN CARRYING EXPLOSIVES: This would include any explosive device that can be transported by a person, including the suicide vest, backpack, satchel charge, etc. Naturally, this limits the size and weight of the device, and therefore, its effective power.

3) VEHICLE BORNE EXPLOSIVES: Cars and trucks packed with explosives are limited to size and weight only by the selected vehicle's carrying capacity.

2 OFTEN OVERLOOKED PHYSICAL SECURITY ELEMENTS & CONCEPTS

SACRAFICIAL AREA(S): It is much too common to see security checkpoints in locations that – themselves – are within or a part of the area to be protected. Conducting search and screening activities WITHIN the lobby area of a hotel is a frequently encountered example. One must always consider that there is nothing to prevent the terrorist from initiating the attack at the security checkpoint and this applies to all 3 of the aforementioned strategies. The location selected to initiate the security measures (i.e. a portal through the secured perimeter) must be considered as UNAVOIDABLY "sacrificial". This area and the people within it will be lost, and would have been lost had the checkpoint been positioned in the wrong place anyway. Preventing the potential threat and losses from reaching the larger target should be the objective of ALL security checkpoints of any type. For small volume traffic think about a measure that airports once considered if it applies to your facilities…that of a separate first screening facility at good distance from the terminal building. Some thought intuitively that this was a good idea because so many people were congregated at the ticket lines, security lines, check-in, etc. The hole in this concept is that in high traffic applications, the crowds of people were merely RELOCATED to the remote screening facility, which then became the new target.

EFFECTIVE PHYSICAL BARRIERS: *A client once had a vehicle security checkpoint where inbound vehicles entered on one side of the gate house, and exited on the other. Seeing the recommended security measures to prevent vehicles from entering through the exit side, the client said "That side is ONE-WAY for exiting only".* Again, terrorists are not bound by ANY rules beyond the laws of physics. It would seem intuitive that those 4" steel pipe barrier arms that are raised and lowered at checkpoints are NOT going to stop a determined adversary driving even the smallest car. The people that actually obey traffic signs and traffic devices – for example - are NOT the ones that pose the threat! Every security checkpoint should be configured to PHYSICALLY prevent an adversary from reaching their target unless they have first been cleared and authorized. Ideally, this step of releasing such a barrier should be performed by someone stationed beyond that barrier and reasonably protected against being forced to open the portal or being otherwise neutralized, even if the attack is initiated at the checkpoint.

A PRACTICAL FOCUS ON EXPLOSIVE BLAST

A bombing by terrorists tends to be more dramatic and news-worthy than most any other strategy. There can be a considerable amount of highly specialized science and engineering involved in many aspects of blast protection, particularly when looked at the worst case scenario….structural collapse. Retaining specialized engineering firms with the latest software can sometimes be necessary.

Short of that expense, there are many aspects of blast protection that security professionals can learn, understand and apply to most situations. One of the best starting points for this self-education might be EXPLOSIVE BLAST – CHAPTER 4 of FEMA guide 428 here;

https://wbdg.org/ccb/DHS/ARCHIVES/fema428_2003.pdf

The guide offers simplified descriptions – with many illustrations – of issues related to the practical effects of blasts. For example, it offers some guidance regarding explosive charge weight relative to distances from the target. Since flying glass (both internally and externally) is one of the major causes of death and injury in a blast, a basic understanding will help responsible professionals in determining how much emphasis and investment should be made in the area of windows and doors.

THE VISITOR, CUSTOMER AND GUEST "EXPERIENCE"

Smart, well-managed business establishments rightly place a high priority on their customers' satisfaction. The hospitality industry is a good example. Sometimes, security measures are viewed as "an inconvenience" to these customers that detracts from customer satisfaction….and sometimes that's true. The opposite can also be true (see our Case Studies at http://www.minieriassociates.com/CASES.htm) regarding some hotel clients. Establishments that are "open to the public" (see this even for example http://edition.cnn.com/2016/01/14/asia/jakarta-gunfire-explosions/) require a particular expertise in order to achieve a proper BALANCE between security and operation of the core business. Experience with such projects along with some creativity will often result in measures that both sides, and the customer, can live with easily.

CORPORATE GOVERNANCE, RESPONSIBILITY AND DUE DILIGENCE

Many organizations have competent security professionals in leadership positions within a global enterprise. Given the practical impact of numerous facility locations, their geographical distances and the varying levels of potential threat in each location, it can be challenging to effectively transfer this expertise down line. The terrorist threat is growing and the need to prepare may never have been greater than it is today. As this is "Anti-Terrorism Security 101" a top tier outline of the appropriate steps for any global enterprise might be as follows;

1) SECURITY MASTER PLAN
2) SECURITY POLICIES, PROCEDURES AND GUIDELINES DOCUMENT
3) PRIORITIZED IMPLEMENTATION PLAN
4) COMPLIANCE AUDITING CYCLE FOR INTERNAL AND 3^{RD} PARTY EXTERNAL AUDITS

ABOUT THE AUTHOR

Michael Minieri started a lifelong career in the security profession in 1974 and is the Principal Security Consultant with Minieri Associates Worldwide Security Consultants. He holds numerous professional credentials including CPP, CSC CST, CCO, CPOI, CFPS, CSM, CET, RAM and more. A leading security magazine called him "…*one of the most prominent people in the industry*…" in an exclusive interview and cover story. Complete information and contact details can be found at www.MinieriAssociates.com